SAFETY/SECURITY PRACTICES - CALL FOR REVIEW

1. Introduction

The Federal Aviation Administration (FAA) and the Office of the Under Secretary of Defense (OSD) are sponsoring a joint effort with the objective of identifying best safety and security practices for inclusion in the two integrated CMMs:

- FAA integrated Capability Maturity Model® (FAA-iCMM® or iCMM) version 2.0 (available at www.faa.gov/aio), and
- Capability Maturity Model Integration^{sm} for Systems Engineering, Software Engineering, Integrated Product and Process Development, and Supplier Sourcing (CMMI^{sm}-SE/SW/IPPD/SS or CMMI) version 1.1 (available at www.sei.cmu.edu)

This project is being co-managed by FAA Chief Engineer for Process Improvement and OSD (AT&L) Defense Systems Directorate, Deputy Director for Software Intensive Systems, with broad participation from government and industry.

We have progressed to the point where we are requesting external review of the preliminary set of practices that have been developed by the project team. Your participation is much appreciated!

This document includes the following information:

- Project Overview
- Instructions for Reviewers
- The Review Package
- List of Project Team Members

2. Project Overview

Safety and security are critical to DoD and FAA, as well as other government and industry organizations. Both CMMI and iCMM provide process improvement frameworks in which safety and security activities can take place. Yet some practices specific to safety and security are not necessarily addressed in these models. The FAA approved a project to include both safety and security in the iCMM, and the CMMI Steering Group had discussed addressing safety and security. In light of similar needs, FAA and DoD decided to collaborate on developing safety/security extensions to both iCMM and CMMI, the intent being that common content would be included in both models.

The following provides a brief overview of project activities and status to date.

- Launch Project – This project was launched in May 2002 with a full day kick-off meeting explaining project background and objectives.

- Form Teams – In June, the following teams were formed: (see team member list on page 8)
  - Project Management – co-leads with overall project responsibility
  - Safety Team – co-leads, authors, and buddies (for peer review), responsible for safety best practices

- Security Team – co-leads, authors, and buddies (for peer review), responsible for security best practices
- Model Team – responsible for author guidelines, providing knowledge of iCMM and CMMI, and editing and integrating common content into the iCMM and CMMI
- Harmonization Team –harmonize safety and security practices seeking common vocabulary
- External Reviewers – provide feedback on interim work products
- Pilot Team – help plan and perform pilot appraisals

- Decide Sources - *Source* documents and *reference* documents for each area (i.e., for safety, and for security) were selected.
  Note: Source documents are the documents from which the proposed model extension practices are derived; mapping of safety and security extension practices to source practices is required; complete coverage of source documents will be demonstrated (note many of these practices may already be contained in CMMI or iCMM, for example those pertaining to configuration management); only major, essential, widely recognized documents are identified as *source* documents (3 to 5 source documents). *Reference* documents are identified as useful in developing best practice in certain areas, but full coverage and detailed mapping is not required.

  The following source documents were selected:

  For Safety: MIL-STD-882C: System Safety Program Requirements
  IEC 61508: Functional Safety of Electrical/Electronic/Programmable Electronic Systems
  DEF STAN 00-56: Safety Management Requirements for Defence Systems

  For Security: ISO 17799: Information Technology – Code of practice for information security management
  ISO 15408: The Common Criteria (v2.1) Mapping of Assurance Levels and Families
  Systems Security Engineering CMM (SSE-CMM) (v2.0)
  NIST 800-30: Risk Management Guide for Information Technology Systems

- Align Source Content and Develop Practices – Agreed source documents were mapped together and aligned according to common subject matter areas, and practices were synthesized from similar practices/ clauses/ activities pertaining to common outcomes. Mappings of all synthesized practices were maintained to the source material.

- Harmonize – Initial harmonization of the safety and security components occurred in October 2002. Safety and security practices were harmonized into a single set of practices referred to as “Integrity Assurance” practices. (See pages 5-7). Mapping is maintained to the original safety and security source documents.

- Distribute for External Review - Distribute harmonized practices for external review. This is where we are now! (*Note:* This activity had been planned to follow our presentation "Integrity Assurance: Extending the CMMI and iCMM for Safety and Security" that was delivered at the *2nd Annual CMMI Technology Conference and User Group*, held 11-14 November in Denver, Colorado.)

Next Steps

- Disposition Change Requests/Revise: (Target – January-February 2003)
  Review comments will be collected, consolidated, and incorporated.

- Integrate the harmonized practices into iCMM and CMMI (Target – February 2003)
  Integrity assurance material will be integrated into the respective models.

- Train on Extensions; Perform Pilot Appraisals: (Target – Spring 2003)
  Pilot appraisals are planned to validate the practices in the context of both iCMM and CMMI. Either the FAA-iCMM Appraisal Method (FAM) or SCAMPI may be used for the pilots. Appraisal teams will be trained on the extended practices.

- Publish: (Target – June 2003)
  A Technical Note will be published describing the Integrity Assurance extensions and their integration into the reference models, with guidance material and mappings to the source material. Revisions based on pilots will be incorporated, as appropriate.

3. Instructions for Reviewers

The Practices: This review package contains the 26 harmonized integrity assurance practices developed according to the project steps outlined above, and using the source documents listed above. The practices are presented in 8 groups for ease of interpretation, and they are numbered within those groups for ease of reference during this review. Only the practice statements are provided in this package, although considerable explanatory information will accompany the final product. However at this time, we need your feedback on whether these practices "seem right" to you. We would like your opinions regarding the following:

- Do these practices reflect and capture your expert experience in implementing safety and/or security activities?
- Are the terminology and structure clear and appropriate?
- Are any essential safety or security practices omitted? (Please elaborate)
- Are there practices included which you do not consider essential? (Please elaborate)
- Do you think these practices also pertain to other specialty fields (such as reliability, dependability, or others)? Could/should they be generalized to incorporate other such disciplines?

Please reference any standards or other source documents (if possible) when elaborating on omissions and relating to other specialty fields.

General notes on the practices:

- For reviewers not familiar with CMMs, please note that practices in a CMM are intended to indicate *what* must be done, but not *how* to do it, nor *who* is to do it. Example methods or techniques or other guidance will be provided in informative material.
- For reviewers familiar with CMMs, please note that we realize some of these practices may already be contained in either CMMI or the iCMM, or they may relate to practices that are already in those models. Placement of the integrity assurance material in the respective models will be carried out later, by the Model Team, after consensus on the practices themselves. Although all comments are welcome, we are not specifically interested in comments regarding overlap of content at this time.

Other Feedback: Of course we welcome any other feedback you might have regarding any aspects of this project. Also, please let us know if you wish to participate further, for example in pilot appraisals.

Terminology and definitions: In harmonizing the safety and security practices developed by the separate security and safety teams, the following definitions were used. Our intent was to use applicable international standard terminology when possible. Please keep these definitions in mind as you review the practices in this package.

- *Integrity Level:* A denotation of a range of values of a property of an item necessary to maintain system risks within tolerable limits. For items that perform mitigating functions, the property is the reliability with which the item must perform the mitigating function. For items whose failure can lead to a threat, the property is the limit on the frequency of that failure. [ISO/IEC 15026, 3.9]
  "The system integrity level corresponds to the tolerable level of risk that is associated with the system. A system can be associated with risk because its failure can lead to a threat, or because its functionality includes mitigation of consequences of initiating events in the system's environment that can lead to a threat." [ISO/IEC 15026, 6.]
- *Threat:* A state of the system or system environment which can lead to adverse effect in one or more given risk dimensions. [ISO/IEC 15026, 3.21]
- *Risk Dimension:* A perspective from which risk assessment is being made for the system (eg safety, economic, security). [ISO/IEC 15026, 3.12]

Ref: *ISO/IEC 15026 International Standard – System and Software Integrity Levels*

Submission: Please complete your review and submit your comments by 10 January 2003.
Comments may be submitted to: Linda.Ibrahim@faa.gov

Integrity Assurance Practices

1. Establishing the Integrity Assurance Program
This set of practices focuses on establishing and maintaining an integrity assurance program.

1.1: Determine Regulatory Requirements, Legal Requirements and Standards
Identify and document regulatory requirements, legal requirements and standards

1.2: Establish Integrity Assurance Objectives
Establish and maintain integrity assurance objectives that reflect the level of acceptable integrity.

1.3: Establish an Integrity Assurance Organization Structure
Establish and maintain an integrity assurance organization structure, including specifying roles and duties of personnel and groups, providing reporting channels, and ensuring adequate levels of managerial and technical independence.

1.4: Establish an integrity assurance plan
Establish and maintain an integrity assurance plan to achieve overall integrity assurance requirements and objectives.

2. Managing the Integrity Assurance Program
This set of practices focuses on implementing, managing, and improving the integrity assurance program.

2.1: Conduct Reviews of Integrity Assurance Activities
Review the progress of activities relative to the integrity assurance program both periodically and at selected milestones.

2.2: Monitor Integrity Assurance Incidents
Monitor, report, analyze and resolve integrity incidents in order to maintain relevance of integrity assurance analyses.

2.3: Establish and control integrity assurance repository
Establish, maintain, and control a repository for integrity assurance evidence.

2.4: Manage the integrity assurance program
Ensure the integrity assurance program is continuously maintained and managed.

3. Managing Supplier Agreements
These practices are applicable to the acquisition of integrity-related products and services from suppliers.

3.1: Select Suppliers
Select suppliers based on an evaluation of their ability to meet specified integrity requirements and established integrity criteria.

3.2: Establish supplier agreements

Establish agreements using criteria that address integrity requirements.

3.3: Satisfy supplier agreements that include integrity requirements

Execute supplier agreements that include integrity requirements and ensure that integrity assurance is delivered with the product or service.

4. Determining and Applying Integrity Principles

These practices focus on determining and applying appropriate integrity principles throughout the lifecycle.

4.1: Determine Appropriate Integrity Principles, Measures and Tools

Select, define, and document the principles, measures and tools required to address integrity during each phase of the lifecycle.

4.2: Apply Integrity Principles, Measures and Tools

Apply the predetermined principles, measures and tools required to address integrity during each phase of the lifecycle.

5. Identifying Threats

These practices focus on threat identification.

5.1: Identify Likely Sources of Threats

Identify likely sources of threats.

5.2: Document Threats and Incidents

Identify and document potential threats and actual incidents, using an appropriate model of the system as a basis.

6. Analyzing Integrity Risk

These practices pertain to the analysis of integrity risk for identified threats.

6.1: Categorize Threats

For each threat, analyze severity and likelihood.

6.2: Prioritize Threats

Prioritize threats for risk treatment.

6.3: Identify Causal Factors

For each threat, determine causal factors.

6.4: Determine Risk Reduction Strategy

For each threat, determine the risk reduction strategy to achieve an acceptable level of risk.

7. Developing and Allocating Integrity Requirements

These practices focus on developing, allocating and maintaining integrity requirements.

7.1: Develop Integrity Requirements

Develop, document and maintain integrity requirements, including associated integrity levels, to address threats and risk reduction strategies.

7.2: Analyze Integrity Requirements

Analyze integrity requirements to ensure they are adequately specified.

7.3: Allocate Integrity Requirements

Allocate integrity requirements.

7.4: Perform Impact Analysis of Changes

Analyze proposed changes to products or services to determine impact on integrity.

8. Determining Integrity Achievement

These practices pertain to the evaluation of work products and delivered products and services.

8.1: Determine Compliance

Assess the work products and delivered products and services throughout the lifecycle to arrive at a determination of the degree of compliance with integrity requirements achieved.

8.2: Assure Integrity

Assess the work products and delivered products and services throughout the lifecycle to assure integrity assurance objectives, reflecting the acceptable level of integrity, have been achieved.

8.3: Establish and Maintain Integrity Assurance Argument

Establish and maintain an integrity assurance argument and supporting evidence throughout the lifecycle.

Safety/Security Team Members – as of 15 November 2002

Name	**Organization**	**Team/Role**
Ahern, Dennis	Northrop Grumman Electronic Systems	Model Team
Ashford, Matt	Australian Defence Materiel Organisation (DMO)	Safety Co-lead
Bate, Roger	Software Engineering Institute	Model Team
Bridges, Kevin	US Federal Aviation Administration (FAA)	Certification Input
Coblentz, Brenda	US Department of Energy (DOE)	Safety Buddy Pilot Team
Conrad, Ray	Lockheed Martin Air Traffic Mgt (Safety)	Safety Buddy
Cooper, David	Praxis Critical Systems Ltd (UK)	Harmonization Team
Courington, Tim	FAA/TRW	Security Co-lead
Croll, Paul	CSC	Harmonization Lead
Dhami, Sartaj		Security Author
Gill, Janet	US Navy, NAVAIR Software System Safety Lead	Safety Buddy
Henning, Ronda	Harris Corp	Security Co-lead
Horn, Mary	US Federal Aviation Administration (FAA)	Security Buddy
Ibrahim, Linda	US Federal Aviation Administration (FAA)	Project Co-Manager Model Team Lead
Jackson, Tom	Lockheed Martin	Security Buddy
Jarzombek, Joe	US Office of Secretary of Defense (OSD)	DoD Co-Sponsor Project Co-Manager Harmonization Team
Keblawi, Faisal	US Federal Aviation Administration (FAA)	Security Co-Lead
Kemens, Victor	US Federal Aviation Administration (FAA)	Security Buddy
LaBruyere, Larry	FAA/TRW	Pilot Team
Leonette, Martha J.	US Federal Aviation Administration (FAA)	Security Author
Miller, Gerald	FAA/TRW	Security Author
Ming, Lisa	Defense Contract Management Agency	Safety Author
Patel, Raju B.	US Air Force, Wright Patterson AFB	Security Buddy
Pierson, Hal	US Federal Aviation Administration (FAA)	Security Buddy
Pyster, Art	US Federal Aviation Administration (FAA)	FAA Co-Sponsor
Roseboro, Douglas	US Federal Aviation Administration (FAA)	Security Buddy
Sherer, Wayne	US Army, Picatinny Arsenal	Model Team
Simmons, Marty	Lockheed Martin Mission Systems (Security)	Security Buddy
Stamnas, Les	SAIC	Pilot Team
Stroup, Ron	US Federal Aviation Administration (FAA)	Safety Co-lead
Stuart, Sandra	US Federal Aviation Administration (FAA)	Security Buddy
Terry, Ray C	US Navy, NAVAIR Systems Safety Division Head	Safety Buddy
VanBuren, Scott	US Federal Aviation Administration (FAA)	Harmonization Team
Wells, Curt	i-Metrics	Model Team
Wetherholt, Martha	NASA	Safety Author